The digraphs from finite fields*

Yangjiang Wei[†], Gaohua Tang
School of Mathematical Sciences, Guangxi Teachers Education University,
Nanning 530023, China

Abstract. For a finite field $\mathbb{F}_{p^t}$ of order p^t, where p is a prime and $t \geqslant 1$, we consider the digraph $G(\mathbb{F}_{p^t}, k)$ that has all the elements of $\mathbb{F}_{p^t}$ as vertices and a directed edge $E(a,b)$ if and only if $a^k = b$, where $a, b \in \mathbb{F}_{p^t}$. We completely determine the structure of $G(\mathbb{F}_{p^t}, k)$, the isomorphic digraphs of $\mathbb{F}_{p^t}$ and the longest cycle in $G(\mathbb{F}_{p^t}, k)$.

2010 MSC: 05C05; 11A07;13M05
Keywords: digraph; component; isomorphic digraphs

1 Introduction

Let $\mathbb{F}_{p^t}$ be a finite field of order p^t, where p is a prime and t is a positive integer, the graph $G(\mathbb{F}_{p^t}, k)$ (k is a positive integer) is a digraph whose set of vertices is all the elements of $\mathbb{F}_{p^t}$ and for which there is a directed edge $E(a,b)$ from $a \in \mathbb{F}_{p^t}$ to $b \in \mathbb{F}_{p^t}$ if and only if $a^k = b$. The digraph $G(\mathbb{Z}_n, k)$ associated with powers modulo n, has been studied in [1]—[3] and [5]—[6]. In this paper, we will generalize some results which were presented in [2], [3] and [6] from prime fields $\mathbb{Z}_p$ to finite fields $\mathbb{F}_{p^t}$.

A *component* of a digraph is a directed subgraph which is a maximal connected subgraph of the associated undirected graph. Suppose α is a vertex of a digraph, the in-degree of α, denoted by $indeg(\alpha)$, is the number of directed edges coming into α. Cycles of length t are called t-cycles and are assumed to be oriented counterclockwise. α is said to be at

*This research was supported by the Guangxi Natural Science Foundation (2011GXNSFA018139, 2010GXNSFB013048, 0991102), Guangxi New Century 1000 Talents Project and the Scientific Research Foundation of Guangxi Educational Committee (200911LX284, 201012MS140).
†Corresponding author: weiyangjiang2004@yahoo.com.cn.

height h, $h \geqslant 0$, if h is the minimal nonnegative integer such that α^{k^h} is a cycle vertex. Moreover, F_α^G refers to the tree attached to the cycle vertex α of the digraph G.

2 The structure of digraphs of cyclic groups

It is well known that the unit group of a finite field $\mathbb{F}_{p^t}$ is a cyclic group C_{p^t-1} of order p^t-1, and we denote the set of nonzero elements of $\mathbb{F}_{p^t}$ by $\mathbb{F}_{p^t}^*$. Hence, $\mathbb{F}_{p^t}^* \cong C_{p^t-1}$. In this section, we investigate the structure of digraphs $G(C_n, k)$ of cyclic groups C_n. Throughout this paper, we denote $C_n = \langle a \rangle$ with the order of a is $o(a) = n$, and let e be the identity of C_n.

Theorem 2.1. [4] *Let $n = uv$, where u is the largest divisor of n relatively prime to k. Suppose* $\gcd(n,k) = d$. *Then in $G(C_n, k)$, we have*

(1) *For $a^x \in C_n$, indeg$(a^x) > 0$ if and only if $d|x$.*

(2) *If $d|x$, then indeg$(a^x) = d$.*

(3) *$G(C_n, k)$ has exactly one component if and only if $q|k$ for any prime divisor q of n.*

(4) *The element α is a cycle vertex in $G(C_n, k)$ if and only if* $\gcd(o(\alpha), k) = 1$, *if and only if $o(\alpha)|u$.*

(5) *The number of all cycle vertices in $G(C_n, k)$ is equal to u.*

(6) *Let α be a cycle vertex in $G(C_n, k)$. Then $F_\alpha^{G(C_n,k)} \cong F_e^{G(C_n,k)}$.*

Theorem 2.2. *Let $n > 1$.*

(1) *Suppose* $\gcd(n,k) = 1$. *Then $G(C_n, k)$ is the disjoint union*

$$G(C_n, k) = \bigcup_{d|n} \underbrace{(\sigma(\text{ord}_d k) \cup \cdots \cup \sigma(\text{ord}_d k))}_{\varphi(d)/\text{ord}_d k},$$

where $\sigma(l)$ is the cycle of length l, $\varphi(d)$ is the Euler totient function.

(2) *Suppose* $\gcd(n,k) > 1$, *$n = uv$, where u is the largest divisor of n relatively prime to k. Then*

$$G(C_n, k) = \bigcup_{d|u} \underbrace{(\sigma(\text{ord}_d k, F_e^{G(C_v,k)}) \cup \cdots \cup \sigma(\text{ord}_d k, F_e^{G(C_v,k)}))}_{\varphi(d)/\text{ord}_d k},$$

where $\sigma(l, F_e^{G(C_v,k)})$ consists of a cycle of length l with a copy of the tree $F_e^{G(C_v,k)}$ attached to each vertex.

Proof. (1) Let $C_n = \bigcup_{d|n} H_d$, where H_d is the set of elements with order d in C_n, $d|n$. Since $\gcd(n,k)=1$, we have $\gcd(d,k)=1$ and $\text{ord}_d k \geqslant 1$ for $d|n$. So for $g \in H_d$, $\text{ord}_d k$ is the least positive integer such that $g^{k^{\text{ord}_d k}} = g$. This implies that each H_d is the disjoint union of cycles of length $\text{ord}_d k$. Moreover, by $|H_d| = \varphi(d)$ we have the formula.

(2) By Theorem 2.1 (4), for $\alpha \in C_n$, α is a cycle vertex of $G(C_n,k)$ if and only if $o(\alpha)|u$. Let H_d be the set of elements with order d in C_n, $d|u$. By the similar argument of (1) above, we derive that each H_d is the disjoint union of $\varphi(d)/\text{ord}_d k$ cycles of length $\text{ord}_d k$.

By Theorem 2.1 (3), $G(C_v,k)$ has exactly one component. Now suppose $Com(e)$ is the component of $G(C_n,k)$ containing the identity e. If we can show $G(C_v,k) \cong Com(e)$, then by Theorem 2.1 (6), the formula holds. In fact, let $C_n = \langle a \rangle$, $o(a) = n$, while $C_v = \langle b \rangle$, $o(b) = v$. If a^x is a vertex of $Com(e)$, then $(a^x)^{k^j} = e$ for some integer j. Hence, $n|xk^j$, i.e., $uv|xk^j$. Moreover, since $\gcd(u,k)=1$, we have $u|x$. Conversely, suppose $x = ux_1$. Since $q|k$ for any prime divisor of v, there exists a positive integer h such that $v|k^h$. Hence, $uv|uk^h$ and so $uv|ux_1k^h$, i.e., $n|xk^h$. Thus we have $(a^x)^{k^h} = e$. So we can conclude that a^x is a vertex of $Com(e)$ if and only if $u|x$. Now let $H = \{a^{um} \,|\, m = 1,\ldots,v\}$. Then $\alpha \in Com(e)$ if and only if $\alpha \in H$. It is easy to show that $H = \langle a^u \rangle$. So H is a subgroup of C_n. Moreover, since $|H| = v$, we have $H \cong C_v$. Therefore, $G(C_v,k) \cong Com(e)$. □

Corollary 2.3. (1) *For $t \geqslant 1$, $G(C_{k^t},k)$ is a complete k-ary tree of height t with the root in e.*

(2) *If $n = k^t m$, where $\gcd(m,k)=1$, $m>1$, $t \geqslant 1$, then*

$$G(C_n,k) = \bigcup_{d|m} \underbrace{(\sigma(\text{ord}_d k, F_e^{G(C_{k^t},k)}) \cup \cdots \cup \sigma(\text{ord}_d k, F_e^{G(C_{k^t},k)}))}_{\varphi(d)/\text{ord}_d k}.$$

3 Isomorphic digraphs of cyclic groups

In this section we give a sufficient and necessary condition for which $G(C_n,k_1) \cong G(C_n,k_2)$. We will show in the following theorem that if n is fixed, only finitely many distinct digraphs result as k varies.

Theorem 3.1. *$G(C_n,k_1) = G(C_n,k_2)$ if and only if $n|k_1 - k_2$.*

Proof. Suppose $G(C_n, k_1) = G(C_n, k_2)$. Then $(a^x)^{k_1} = (a^x)^{k_2}$ for $x = 1, \ldots, n$. Hence, $n|k_1 - k_2$. Conversely, assume that $n|k_1 - k_2$, then $a^{k_1} = a^{k_2}$ and hence $(a^x)^{k_1} = (a^x)^{k_2}$ for $x = 1, \ldots, n$, which implies that $G(C_n, k_1) = G(C_n, k_2)$. This completes our proof. □

Lemma 3.2. (1) *Suppose that $q|n$ if and only if $q|k$, where q is prime. Let m be a positive integer, and* $\gcd(n, m) = 1$. *Then* $G(C_n, k) \cong G(C_n, km)$.

(2) *Suppose that* $\gcd(n, k_1) = \gcd(n, k_2)$. *Moreover, $q|n$ if and only if $q|k_1$, if and only if $q|k_2$, where q is prime. Then there exists $m \geqslant 1$ and* $\gcd(n, m) = 1$ *such that* $k_2 \equiv k_1 m \pmod{n}$.

Proof. (1) Let $E(G(C_n, k))$ be the set of edges of $G(C_n, k)$ and $E(a, b)$ the directed edge from vertex a to vertex b. We define $f : E(G(C_n, k)) \to E(G(C_n, km))$ by $f(E(a^x, a^{kx})) = E(a^{mx}, a^{km^2 x})$ for $a^x \in C_n$.

Firstly, we will check that f is one-to-one and onto. Suppose $a^{mx_1} = a^{mx_2}$, then $n|m(x_1 - x_2)$. Since $\gcd(n, m) = 1$, we have $n|x_1 - x_2$. Hence, $a^{x_1} = a^{x_2}$. Therefore, f is one-to-one. On the other hand, since $\gcd(n, m) = 1$, if $1 \leqslant y \leqslant n$, there exists a unique integer x_0 $(1 \leqslant x_0 \leqslant n)$ satisfing $mx_0 \equiv y \pmod{n}$. Hence, $f(E(a^{x_0}, a^{kx_0})) = E(a^y, a^{kmy})$. So f is onto $G(C_n, km)$.

Second, by Theorem 2.1 (3), both $G(C_n, k)$ and $G(C_n, km)$ have exactly one component, respectively. We will show that the height of a^{kx} in $G(C_n, k)$ is h if and only if the height of $a^{km^2 x}$ in $G(C_n, km)$ is h. Let the height of a^{kx} in $G(C_n, k)$ be h, then h is the least positive integer such that $(a^{kx})^{k^h} = e$. Thus $(a^{km^2 x})^{(km)^h} = e$. If $(a^{km^2 x})^{(km)^{h-1}} = e$, then $(a^{k^h x})^{m^{h+1}} = e$. Since $\gcd(n, m) = 1$, we have $a^{k^h x} = e$, i.e., $(a^{kx})^{k^{h-1}} = e$, which implies that the height of a^{kx} in $G(C_n, k)$ is $h - 1$, which is a contradiction. Hence, the height of $a^{km^2 x}$ in $G(C_n, km)$ is also h. Similarly, we can check that if the height of $a^{km^2 x}$ in $G(C_n, km)$ is h, then the height of a^{kx} in $G(C_n, k)$ is also h.

Finally, we will show that $(a^{kx_1})^{k^j} = (a^{kx_2})^{k^j}$ if and only if $(a^{km^2 x_1})^{(km)^j} = (a^{km^2 x_2})^{(km)^j}$, for $j \geqslant 0$. On the one hand, by $(a^{kx_1})^{k^j} = (a^{kx_2})^{k^j}$, we derive that $n|k^{j+1}(x_1 - x_2)$. Thus $n|k^{j+1} m^{j+2}(x_1 - x_2)$, therefore $(a^{km^2 x_1})^{(km)^j} = (a^{km^2 x_2})^{(km)^j}$. On the other hand, by $(a^{km^2 x_1})^{(km)^j} = (a^{km^2 x_2})^{(km)^j}$, we have $n|k^{j+1} m^{j+2}(x_1 - x_2)$. It is clear $n|k^{j+1}(x_1 - x_2)$ because $\gcd(n, m) = 1$, hence $(a^{kx_1})^{k^j} = (a^{kx_2})^{k^j}$.

By the above argument, we can conclude that $G(C_n, k) \cong G(C_n, km)$.

(2) By hypothesis, let $n = p_1^{t_1} \cdots p_s^{t_s}$, $k_1 = p_1^{\lambda_1} \cdots p_\sigma^{\lambda_\sigma} p_{\sigma+1}^{x_{\sigma+1}} \cdots p_s^{x_s}$, $k_2 = p_1^{\lambda_1} \cdots p_\sigma^{\lambda_\sigma} p_{\sigma+1}^{y_{\sigma+1}} \cdots p_s^{y_s}$, where $p_1, \ldots, p_s$ are distinct primes, and for $i = 1, \ldots, \sigma$, $1 \leqslant \lambda_i < t_i$, while for $j = \sigma+1, \ldots, s$, $x_j \geqslant t_j \geqslant 1$ and $y_j \geqslant t_j$. Since $\gcd(p_1 \cdots p_\sigma, p_{\sigma+1} \cdots p_s) = 1$, there exists a positive integer m_0 such that

$$p_{\sigma+1}^{x_{\sigma+1}-t_{\sigma+1}} \cdots p_s^{x_s - t_s} m_0 \equiv p_{\sigma+1}^{y_{\sigma+1}-t_{\sigma+1}} \cdots p_s^{y_s - t_s} \pmod{p_1^{t_1} \cdots p_\sigma^{t_\sigma}}.$$

Clearly, $p_i \nmid m_0$ for $i = 1, \ldots, \sigma$.

If $p_j \nmid m_0$ for $j = \sigma + 1, \ldots, s$, let $m = m_0$, then $\gcd(n, m) = 1$ and $k_2 \equiv k_1 m \pmod{n}$. If there exists a nonempty subset B of $A = \{\sigma+1, \ldots, s\}$ such that $p_i | m_0$ for $i \in B$, while $p_j \nmid m_0$ for $j \in A \setminus B$, let $m = m_0 + p_1^{t_1} \cdots p_\sigma^{t_\sigma} \prod_{j \in A \setminus B} p_j$. Then we have $\gcd(n, m) = 1$ and $k_2 \equiv k_1 m \pmod{n}$, as desired. □

Theorem 3.3. *$G(C_n, k_1) \cong G(C_n, k_2)$ if and only if the following two conditions are satisfied.*

(1) $\gcd(n, k_1) = \gcd(n, k_2)$.

(2) *There exists a positive integer u such that $n = uv$, u is the largest divisor of n relatively prime to k_1 and is also the largest divisor of n relatively prime to k_2. Moreover, for any $d|u$, $\mathrm{ord}_d k_1 = \mathrm{ord}_d k_2$.*

Proof. If $\gcd(n, k_1) = 1$, by Theorem 2.2 (1), the proof is clear. In the following, assume that $\gcd(n, k_1) > 1$.

Firstly, we prove the necessity of this theorem. Suppose $G(C_n, k_1) \cong G(C_n, k_2)$. By Theorem 2.1 (1) and (2), we have $\gcd(n, k_1) = \gcd(n, k_2)$. If $n = uv$ and u is the largest divisor of n relatively prime to k_1, it is easy to check that u is also the largest divisor of n relatively prime to k_2 because $\gcd(n, k_1) = \gcd(n, k_2)$. Furthermore, by Theorem 2.1 (2), $G(C_u, k_1) \cong G(C_u, k_2)$. Hence, for any $d|u$, $\mathrm{ord}_d k_1 = \mathrm{ord}_d k_2$.

Conversely, suppose $\gcd(n, k_1) = \gcd(n, k_2)$ and for any $d|u$, $\mathrm{ord}_d k_1 = \mathrm{ord}_d k_2$. By Theorem 2.2 (1), we derive that $G(C_u, k_1) \cong G(C_u, k_2)$. Moreover, since $\gcd(u, v) = 1$, we have $\gcd(v, k_1) = \gcd(v, k_2)$ and $q|k_1$, $q|k_2$ for any prime divisor of v. We can assume that $v = p_1^{t_1} \cdots p_s^{t_s}$ and

$$k_1 = k_1' m_1, where\ k_1' = p_1^{\lambda_1} \cdots p_\sigma^{\lambda_\sigma} p_{\sigma+1}^{x_{\sigma+1}} \cdots p_s^{x_s}, \gcd(v, m_1) = 1,$$

$$k_2 = k_2' m_2, where\ k_2' = p_1^{\lambda_1} \cdots p_\sigma^{\lambda_\sigma} p_{\sigma+1}^{y_{\sigma+1}} \cdots p_s^{y_s}, \gcd(v, m_2) = 1,$$

$p_1, \ldots, p_s$ are distinct primes, and for $i = 1, \ldots, \sigma$, $1 \leqslant \lambda_i < t_i$, while for $j = \sigma + 1, \ldots, s$, $x_j \geqslant t_j \geqslant 1$ and $y_j \geqslant t_j$. By Lemma 3.2 (1), $G(C_v, k_1) = G(C_v, k_1' m_1) \cong G(C_v, k_1')$ and $G(C_v, k_2) = G(C_v, k_2' m_2) \cong G(C_v, k_2')$. Moreover, by Lemma 3.2 (2), there exists a positive integer m such that $\gcd(m, v) = 1$ and $k_2' \equiv k_1' m \pmod{v}$. Using Theorem 3.1, $G(C_v, k_2') = G(C_v, k_1' m) \cong G(C_v, k_1')$. Therefore, $G(C_v, k_1) \cong G(C_v, k_2)$. Hence, by Theorem 2.2 (2), we can conclude that $G(C_n, k_1) \cong G(C_n, k_2)$. □

For example, $G(C_8, 3) \cong G(C_8, 7)$, $G(C_8, 2) \cong G(C_8, 6)$. See Fig. 1—4.

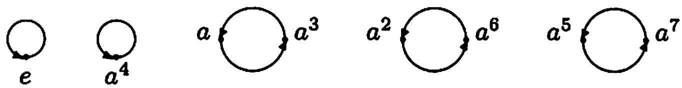

Fig. 1. The digraph $G(C_8, 3)$

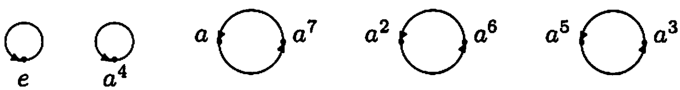

Fig. 2. The digraph $G(C_8, 7)$

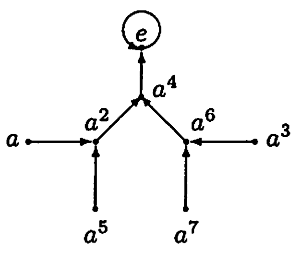

Fig. 3. The digraph $G(C_8, 2)$

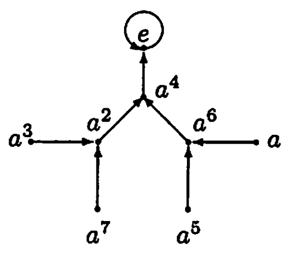

Fig. 4. The digraph $G(C_8, 6)$

4 Occurrence of long cycles in $G(\mathbb{F}_{p^t}, k)$

In this section we provide an upper bound for the cycle lengths appearing in $G(\mathbb{F}_{p^t}, k)$.

Theorem 4.1. *If $p^t - 1$ is a power of 2, i.e., $p^t - 1 = 2^s$, $s \geqslant 1$. Then*

(1) $(p,t,s)=(3,2,3)$ *or* $(2^{2^r}+1,1,2^r)$, *where* $2^{2^r}+1$ *is a Fermat prime,* $r\geqslant 1$.

(2) *Let* $p=2^{2^r}+1>5$ *be a Fermat prime. Then the length of the longest cycle in* $G(\mathbb{F}_p,k)$ *is less than or equal to* $\frac{p-1}{4}$. *Moreover,* $G(\mathbb{F}_p,k)$ *contains a cycle of length* $\frac{p-1}{4}$ *if and only if* $\mathrm{ord}_{2^{2^r}}k=\frac{p-1}{4}$.

Proof. (1) Suppose that $t\geqslant 3$. If $t\geqslant 3$ is odd, since $p^t-1=(p-1)(p^{t-1}+\cdots+p+1)$ and clearly $p^{t-1}+\cdots+p+1>1$ is odd, we have p^t-1 is not a power of 2 when $t\geqslant 3$ is odd. If $t\geqslant 3$ is even, let $t=2h$, $h>1$. Since $p^t-1=p^{2h}-1=(p^h+1)(p^h-1)$, we derive that p^t-1 is not a power of 2 when $t\geqslant 3$ is even. So $t\leqslant 2$ and it is easy to derive the result.

(2) Since $p=2^{2^r}+1>5$, $r\geqslant 2$. If $2|k$, by Theorem 2.1 (3), $G(\mathbb{F}_p^*,k)$ contains exactly one component with a 1–cycle. We know we are not interested in longest cycles of length 1. Now suppose $2\nmid k$, then by Theorem 2.2 (1), the length of each cycle in $G(\mathbb{F}_p^*,k)$ is $\mathrm{ord}_d k$, where $d|p-1$. Clearly $\mathrm{ord}_d k|\mathrm{ord}_{p-1}k$. Hence the maximal length of cycles is $\mathrm{ord}_{p-1}k=\mathrm{ord}_{2^{2^r}}k$. However, $\mathbb{Z}_{2^{2^r}}^*$ does not have a primitive root for $r\geqslant 2$. Thus $\mathrm{ord}_{2^{2^r}}k<\varphi(2^{2^r})=2^{2^r-1}$. Furthermore, since $\mathrm{ord}_{2^{2^r}}k|2^{2^r-1}$, we have $\mathrm{ord}_{2^{2^r}}k\leqslant 2^{2^r-2}=\frac{p-1}{4}$, as desired. □

For example, the length of the longest cycles in $G(\mathbb{F}_{17},k)$ is $\frac{p-1}{4}=4$ if and only if $k=3,5,11,13$.

Theorem 4.2. *Suppose* $p^t>5$ *is not a power of* 2.

(1) *The length of the longest cycle in* $G(\mathbb{F}_{p^t},k)$ *is less than or equal to* $\frac{p^t-3}{2}$.

(2) $G(\mathbb{F}_{p^t},k)$ *contains a cycle of length* $\frac{p^t-3}{2}$ *if and only if* $\frac{p^t-1}{2}$ *is an odd prime, and* k *is a primitive root modulo* p^t-1 *or modulo* $\frac{p^t-1}{2}$, *where* $t=1$, *or* $t\geqslant 3$ *is odd with* $p=3$.

Proof. (1) It is a direct consequence of [4, Proposition 3.17].

(2) Suppose that the length of the longest cycle in $G(\mathbb{F}_{p^t},k)$ is $\frac{p^t-3}{2}$. Let $p^t-1=2^s\tau$, $\tau\geqslant 3$ is odd, $s\geqslant 1$.

Case 1. Let $\gcd(p^t-1,k)=1$. By Theorem 2.2 (1), the length of each cycle in $G(\mathbb{F}_{p^t}^*,k)$ is $\mathrm{ord}_d k$, where $d|p^t-1$. Since $\mathrm{ord}_d k\leqslant\mathrm{ord}_{p^t-1}k\leqslant\varphi(p^t-1)=2^{s-1}\varphi(\tau)<2^{s-1}\tau$, we have $\mathrm{ord}_{p^t-1}k=\varphi(p^t-1)=\frac{p^t-3}{2}$. While $\varphi(p^t-1)=\varphi(2^s\tau)=2^{s-1}\varphi(\tau)$, $\frac{p^t-3}{2}=2^{s-1}\tau-1$, so $s=1$ and $\varphi(\tau)=\tau-1$. Hence, τ is an odd prime. Therefore, $p^t-1=2\tau$ for some odd prime τ. If

$t = 1$, then $\frac{p-1}{2}$ is an odd prime. Moreover, by $\text{ord}_{p-1}k = \frac{p-3}{2}$, we derive that k is a primitive root modulo $p-1$. On the other hand, if $t > 1$ and t is even, let $t = 2r$. Then $2\tau = p^t - 1 = p^{2r} - 1$, which is impossible. Therefore, t is odd if $t > 1$. Moreover, since $\tau = \frac{p^t-1}{2} = \frac{(p-1)(p^{t-1}+\cdots+p+1)}{2}$ is an odd prime, we derive that $p = 3$ and $\frac{3^t-1}{2}$ is an odd prime. By $\text{ord}_{3^t-1}k = \frac{3^t-3}{2}$, k is a primitive root modulo $3^t - 1$.

Case 2. Let $\gcd(p^t - 1, k) > 1$ and $p^t - 1 = uv$, where u is the largest divisor of n relatively prime to k. Since $p^t - 1 > 5$, clearly $v \geqslant 2$. By Theorem 2.2 (2), the length of the longest cycle in $G(\mathbb{F}_{p^t}, k)$ is equal to the length of the longest cycle in $G(C_u, k)$. It is obvious that $v = 2$. Hence $u - 1 = \frac{p^t-3}{2}$. Therefore $G(C_u, k)$ contains exactly two components and so $\varphi(u) = \text{ord}_u k = u - 1$ due to Theorem 2.2 (1). Hence u is an odd prime. So we have $p^t - 1 = 2u$ for some odd prime u. If $t = 1$, then $\frac{p-1}{2}$ is an odd prime. Moreover, by $\text{ord}_{\frac{p-1}{2}}k = \frac{p-3}{2}$, we derive that k is a primitive root modulo $\frac{p-1}{2}$. On the other hand, if $t > 1$, by the similar argument of Case 1 above, we should derive that t must be odd and $p = 3$, as desired.

The sufficiency of this theorem is easy to check. □

For example, the length of the longest cycles in $G(\mathbb{F}_{3^3}, k)$ is $\frac{3^3-3}{2} = 12$ if and only if $k = 2, 7, 11, 15, 18, 19, 20, 24$.

References

[1] W. Carlip, M. Mincheva: Symmetry of iteration digraphs. Czechoslovak Math. J. 58, 131–145 (2008)

[2] C. Lucheta, E. Miller, C. Reiter: Digraphs from powers modulo p. Fibonacci Quart. 34, 226–239 (1996)

[3] T.D. Rogers: The graph of the square mapping on the prime fields. Discrete Math. 148, 317–324 (1996)

[4] M. Sha: Digraphs from endomorphisms of finite cyclic groups. ArXiV, July 10 (2010)

[5] L. Somer, M. Křížek: On a connection of number theory with graph theory. Czechoslovak Math. J. 54 (129), 465–485 (2004)

[6] L. Somer, M. Křížek: On symmetric digraphs of the congruence $x^k \equiv y \pmod{n}$. Discrete Math. 309, 1999–2009 (2009)